

## CLAIMS

Thus, having described the systems and methods for virus checking software code, we claim the following:

1           1.       A method for identifying infected program instructions, comprising the  
2 steps of:

3               inserting a dynamic execution layer interface (DELI) between computing  
4 device hardware and the program instructions;

5               monitoring the program instructions as they enter the DELI to determine if the  
6 code has been previously processed by the computing device hardware; and when it is  
7 the case that the application code has not been previously processed,

8               analyzing the program instructions to determine if program instructions are  
9 infected.

1           2.       The method of claim 1, wherein the step of analyzing the program  
2 instructions comprises an investigation of the contents of instructions within code  
3 fragments.

1           3.       The method of claim 1, wherein the step of analyzing the program  
2 instructions comprises inserting decrypted program instructions into a virus detection  
3 manager.

1           4.       The method of claim 3, further comprising the step of:  
2 releasing program instructions from the virus detection manager when infected  
3 program instructions are not detected.

1           5.       The method of claim 3, wherein the step of analyzing the program  
2 instructions comprises performing a signature comparison with the contents of the  
3 code fragments.

1           6.       The method of claim 3, wherein the step of analyzing the program  
2 instructions comprises monitoring the behavior of the contents of the code fragments  
3 in a virtual computing device.

1           7.       The method of claim 3, wherein the step of analyzing the program  
2 instructions comprises applying a plurality of tests on the contents of the code  
3 fragments in a virtual computing device.

1           8.       The method of claim 4, further comprising the step of:  
2 processing the released program instructions in computer hardware.

1           9.       A system for detecting infected program instructions in active software  
2 applications, comprising:  
3       means for intercepting program instructions;  
4       means for determining when the intercepted program instructions have not  
5 been processed by the computing device; and  
6       means for analyzing the intercepted program instructions that have not been  
7 processed by the computing device prior to forwarding the intercepted program  
8 instructions to computer hardware.

1           10.      The system of claim 9, further comprising:  
2 means for gaining control over execution of program instructions.

1           11.      The system of claim 9, further comprising:  
2 means for executing program instructions.

1           12.      The system of claim 9, wherein the means for intercepting comprises a  
2 dynamic execution layer interface (DELI).

1           13.      The system of claim 9, wherein the means for analyzing the intercepted  
2 program instructions comprises a virus detection manager.

1           14.      The system of claim 13, wherein the virus detection manager  
2 comprises a controller configured to apply a plurality of virus detection tests over the  
3 contents of the intercepted program instructions.

1           15.    A virus detection program stored on a computer-readable medium,  
2 comprising:  
3           logic configured to intercept program instructions;  
4           logic configured to determine if the intercepted program instructions have not  
5 been processed by a computing device; and  
6           logic configured to determine when the intercepted program instructions that  
7 have not been processed by the computing device are infected with a virus.

1           16.    The program of claim 15, further comprising:  
2           logic configured to gain control over execution of intercepted program  
3 instructions.

1           17.    The program of claim 15, further comprising:  
2           logic configured to execute program instructions.

1           18.    The program of claim 15, further comprising:  
2           logic configured to forward non-infected intercepted program instructions to  
3 the computing device.

1           19.    A computer system, comprising:  
2           a processor;  
3           an execution memory;  
4           a dynamic execution layer interface (DELI) residing between at least one  
5 application and the processor, wherein the DELI comprises:  
6                a core configured to cache and execute certain application code  
7 fragments;  
8                an application programming interface configured to provide access to  
9 caching and executing functions of the core to a virus detection manager; and  
10               a system control and configuration layer configured to provide policies  
11 for operation of the core.

1           20.    The system of claim 19, wherein the virus detection manager is  
2 configured to apply at least one virus detection test on the contents of application code  
3 fragments.

1           21.    The system of claim 19, wherein the core is configured to process  
2 executable application code fragments from the at least one application that have not  
3 been previously sent to the processor.

1           22.    The system of claim 21, wherein the virus detection manager controls  
2 whether application code fragments are released to the processor.

1           23.    The system of claim 22, wherein application code fragments that  
2 contain at least one virus signature are not released to the processor.

1           24.    The system of claim 22, wherein application code fragments that  
2 behave in a manner consistent with known virus attacks are not released to the  
3 processor.